

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 08008851 A

(43) Date of publication of application: 12.01.96

(51) Int. Cl
H04H 1/00
H04L 9/00
H04L 9/10
H04L 9/12

(21) Application number: 06134667

(22) Date of filing: 16.06.94

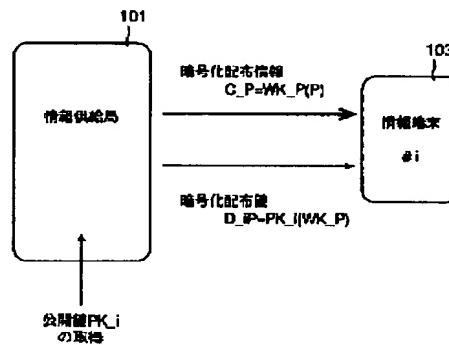
(71) Applicant: TOSHIBA CORP

(72) Inventor: SHINPO ATSUSHI
KAMITAKE TAKASHI
MAEDA KENICHI

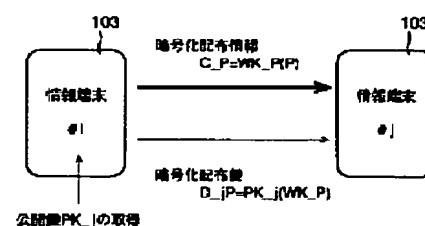
(54) INFORMATION DISTRIBUTION SYSTEM AND INFORMATION DISTRIBUTION METHOD

COPYRIGHT: (C)1996,JPO

(a)



(b)



(57) Abstract:

PURPOSE: To provide an information distribution system capable of performing a primary and a secondary distribution of paid information and preventing damage from reaching equipments other than the terminal equipment even when the physical safety of the terminal is not guaranteed any more.

CONSTITUTION: In this information distribution system for distributing digital information from a supply station 101 to the plural terminals 103 among the terminals 103 through an information transmission medium, the supply station 101 is provided with a means for outputting ciphered information for which the information is ciphered by a first cryptographic key intrinsic to the respective pieces of the information and a distribution key for which a first deciphering key corresponding to the first cryptographic key is ciphered by a second cryptographic key intrinsic to a reception terminal to the medium. The respective terminals 103 are provided with the means for inputting the ciphered information and the distribution key transmitted from the supply station 101 or the other terminal through the medium, the means for deciphering the ciphered information by the first deciphering key extracted by deciphering the distribution key by a second deciphering key corresponding to the second cryptographic key, the means for ciphering the first deciphering key extracted by deciphering the encipherment distribution key by the second deciphering key by the second cryptographic key intrinsic to the terminal which is the transmission destination of the ciphered information and the means for outputting the distribution key obtained by the means and the ciphered information to the medium.

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-8851

(43)公開日 平成8年(1996)1月12日

(51) Int.Cl. ⁶	識別記号	府内整理番号	F I	技術表示箇所
H 04 H 1/00		F		
H 04 L 9/00				
9/10				
9/12				

H 04 L 9/00 Z
審査請求 未請求 請求項の数 8 O L (全 16 頁)

(21)出願番号 特願平6-134667
(22)出願日 平成6年(1994)6月16日

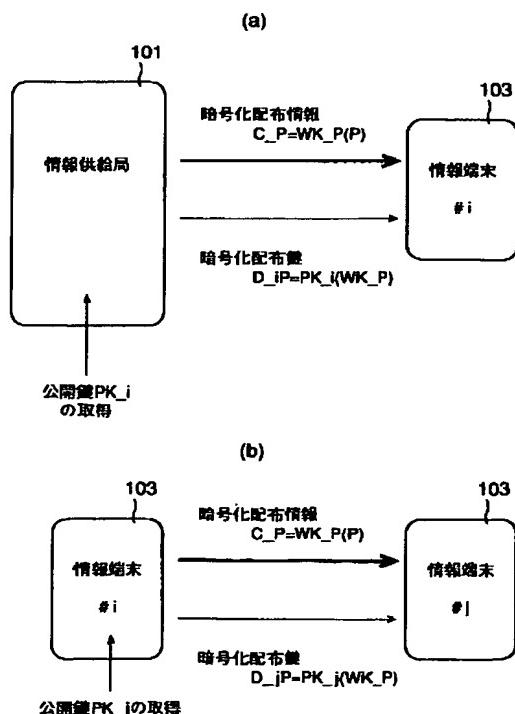
(71)出願人 000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者 新保 淳
神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内
(72)発明者 神竹 孝至
神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内
(72)発明者 前田 賢一
神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内
(74)代理人 弁理士 鈴江 武彦

(54)【発明の名称】情報配布システムおよび情報配布方法

(57)【要約】

【目的】 有料情報の1次・2次配布ができ、端末の物理的安全性が保証されなくなっても被害がその端末装置以外に及ばない情報配布システムを得ること。

【構成】 供給局から複数の端末に及び端末間で情報伝達媒体を介しデジタル情報を配布する情報配布システムにおいて、供給局は、該情報毎に固有の第1暗号鍵で該情報を暗号化した暗号化情報と、受信端末固有の第2暗号鍵で第1暗号鍵に対応する第1復号鍵を暗号化した配布鍵を該媒体に出力する手段を備え、端末夫々は、供給局又は他端末から該媒体を介し伝達された暗号化情報と配布鍵を入力する手段と、第2暗号鍵に対応する第2復号鍵で配布鍵を復号し取出した第1復号鍵で暗号化情報を復号する手段と、暗号化配布鍵を第2復号鍵で復号し取出した第1復号鍵を暗号化情報の伝達先の端末固有の第2暗号鍵で暗号化する手段と、この手段で得た配布鍵と暗号化情報を該媒体に出力する手段を備える。



【特許請求の範囲】

【請求項1】デジタル情報の配布を行う情報供給局と、前記デジタル情報を受ける複数の情報端末と、前記情報供給局および前記複数の情報端末の相互間を接続する情報伝達媒体とから構成されるとともに、各情報端末間では前記情報供給局から配布された前記デジタル情報を2次的に配布する情報配布システムにおいて、前記情報供給局は、

前記デジタル情報ごとに固有に割り当てた第1の暗号鍵を用いて該デジタル情報を暗号化した暗号化デジタル情報と、この暗号化デジタル情報を伝達すべき前記情報端末に固有に割り当てられた第2の暗号鍵を用いて該第1の暗号鍵に対応する第1の復号鍵を暗号化した暗号化配布鍵とを前記情報伝達媒体に出力する手段を備え、

前記情報端末夫々は、

前記情報供給局または他の前記情報端末から前記情報伝達媒体を介して伝達された前記暗号化デジタル情報および前記暗号化配布鍵を入力する入力手段と、

前記第2の暗号鍵に対応する固有の第2の復号鍵を用いて前記暗号化配布鍵を復号した後、この復号により得られる前記第1の復号鍵を用いて前記暗号化デジタル情報を復号する復号手段と、

前記暗号化配布鍵を前記第2の復号鍵を用いて復号した後、この復号により得られる前記第1の復号鍵を、前記暗号化デジタル情報を伝達すべき別の前記情報端末に固有に割り当てられた前記第2の暗号鍵を用いて暗号化する暗号化配布鍵変換手段と、

この暗号化配布鍵変換手段により得られる前記暗号化配布鍵と前記暗号化デジタル情報を前記情報伝達媒体に出力する出力手段とを備えたことを特徴とする情報配布システム。

【請求項2】前記情報端末夫々は、前記復号手段により得られる前記暗号化デジタル情報を編集するための編集手段と、

前記暗号化デジタル情報または前記復号手段により復号されたデジタル情報を利用するごとに更新される利用可能度数情報を格納する利用可能度数情報格納手段と、

前記復号手段による前記暗号化デジタル情報の復号行為および前記編集手段による前記デジタル情報の編集行為に応じた利用情報の記録を生成するとともに、前記復号行為および前記編集行為に応じて前記利用可能度数情報格納手段に格納された前記利用可能度数情報の更新を行う利用管理手段とをさらに備えることを特徴とする請求項1に記載の情報配布システム。

【請求項3】前記復号手段および前記暗号化配布鍵変換手段は、外部から物理的に保護された領域に設けられることを特徴とする請求項1に記載の情報配布システム。

【請求項4】デジタル情報の配布を行う情報供給局

と、前記デジタル情報を受ける複数の情報端末と、前記情報供給局および前記複数の情報端末の相互間を接続する情報伝達媒体とから構成されるとともに、各情報端末間では前記情報供給局から配布された前記デジタル情報を2次的に配布する情報配布システムにおいて、前記情報供給局は、

前記デジタル情報ごとに固有に割り当てた第1の暗号鍵を用いて該デジタル情報を暗号化した暗号化デジタル情報およびこの暗号化デジタル情報を伝達すべき

10 前記情報端末に固有に割り当てられた第2の暗号鍵を用いて該第1の暗号鍵に対応する第1の復号鍵を暗号化した暗号化配布鍵、または該暗号化配布鍵のみを前記情報伝達媒体に出力する手段を備え、
前記情報端末夫々は、

前記情報伝達媒体を介して、前記情報供給局から伝達された前記暗号化デジタル情報および前記暗号化配布鍵または、他の前記情報端末から伝達された前記暗号化デジタル情報および前記情報供給局から伝達された前記暗号化配布鍵を入力する入力手段と、

20 前記第2の暗号鍵に対応する固有の第2の復号鍵を用いて前記暗号化配布鍵を復号した後、この復号により得られる前記第1の復号鍵を用いて前記暗号化デジタル情報を復号する復号手段と、

前記暗号化デジタル情報を前記情報伝達媒体に出力する出力手段とを備えたことを特徴とする情報配布システム。

【請求項5】前記情報供給局は、前記情報端末夫々に対する前記暗号化配布鍵の配布行為を記録する手段をさらに備え、

30 前記情報端末夫々は、前記復号手段により得られる前記暗号化デジタル情報を編集するための編集手段と、前記暗号化デジタル情報または前記復号手段により復号されたデジタル情報を利用するごとに更新される利用可能度数情報を格納する利用可能度数情報格納手段と、
前記復号手段による前記暗号化デジタル情報の復号行為および前記編集手段による前記デジタル情報の編集行為に応じた利用情報の記録を生成するとともに、前記復号行為および前記編集行為に応じて前記利用可能度数情報格納手段に格納された前記利用可能度数情報の更新を行う利用管理手段とをさらに備えることを特徴とする請求項4に記載の情報配布システム。

40 【請求項6】前記復号手段は、外部から物理的に保護された領域に設けられた特徴とする請求項4に記載の情報配布システム。

【請求項7】第1の情報端末が、デジタル情報の配布を受けるとともに、受けたデジタル情報を第2の情報端末に2次的に配布する情報配布方法において、前記デジタル情報ごとに固有に割り当てた第1の暗号鍵を用いて該デジタル情報を暗号化した暗号化デジ

50

タル情報と、前記第1の情報端末に固有に割り当てられた第2の暗号鍵を用いて該第1の暗号鍵に対応する第1の復号鍵を暗号化した暗号化配布鍵とを入力する入力ステップと、

前記第2の暗号鍵に対応する固有の第2の復号鍵を用いて前記暗号化配布鍵を復号する復号ステップと、この復号ステップにより得られる前記第1の復号鍵を、前記第2の情報端末に固有に割り当てられた前記第2の暗号鍵を用いて暗号化する暗号化ステップと、この暗号化ステップにて得られる前記暗号化配布鍵と前記暗号化ディジタル情報を出力する出力ステップとを有することを特徴とする情報配布方法。

【請求項8】第1の情報端末が、ディジタル情報の配布を受けるとともに、受けたディジタル情報を第2の情報端末に2次的に配布する情報配布方法において、前記ディジタル情報ごとに固有に割り当てた第1の暗号鍵を用いて該ディジタル情報を暗号化した暗号化ディジタル情報および前記第1の情報端末に固有に割り当てられた第2の暗号鍵を用いて該第1の暗号鍵に対応する第1の復号鍵を暗号化した暗号化配布鍵を入力する入力ステップと、

前記第2の暗号鍵に対応する固有の第2の復号鍵を用いて前記暗号化配布鍵を復号する処理および前記暗号化ディジタル情報を出力する処理の少なくとも一方を行うステップとを有することを特徴とする情報配布方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、ディジタル化された著作物の流通において、著作者の権利を保証しつつ、利用者はその閲覧および編集が可能となる情報配布システムおよび情報配布方法に関する。

【0002】

【従来の技術】近年のディジタル通信や計算機技術等の発展により、画像・音声・テキストなどの様々な情報をデジタル化し統合的に取り扱うことが可能となりつつある。このような技術は各適用分野で導入が検討されており、例えば情報配布に関する分野では、ディジタル化された新聞、雑誌、音楽、映画、…などの著作物を情報利用者がネットワークを介して受信できるシステムがいくつか提案されている。

【0003】しかしながら、この種の情報配布システムを実際に構築しようとすると、著作権保護という重要な問題が顕在化してくる。すなわち、上記システムで扱うディジタル情報にはアナログ情報にない特徴として、完全な複製を容易に、しかも無尽蔵に作成できる優れた点がある。これは利用者にとって大きな利点であるが、著作物を提供する側にとっては権利保護の面で問題である。従って、上記システムを完全なものにするためには、ディジタル情報の特徴を損なわずにしかも著作権を保護できるような仕組みが必須となるのである。

【0004】このような問題は、有償なディジタル情報のさきがけともいえるソフトウェア（プログラム）の配布において既に発生している。そして、著作権保護を法律による規制に委ねるのみでは自ずと限界があるため、技術的な対策が検討されている。以下、ソフトウェアの配布において著作権保護のために講じられている2つの対策を説明する。

【0005】1つめの方法は、特定の計算機でしか実行できない形式にソフトウェアを変換して配布する方法である。

すなわち、計算機に固有のIDを割り当てるとともに、ソフトウェアの販売時に利用者の計算機IDを販売ソフトに織り込んでおく。ソフトウェアの実行時には、計算機IDとソフトウェア内のIDとを比較し、一致しなければ起動されないようにする。ただし、ソフトウェアの一部に計算機IDコードを書き込むだけでは、その書き込み位置さえ判れば簡単にプロジェクトが破られてしまう。そこで、拡張法として暗号技術を利用し、ソフトウェア全体をある鍵で暗号化しておき、その鍵を個別の計算機ごとにカスタマイズして配布する方法が提案されている。具体的には、次の通りである。計算機には固有の鍵（ここでは端末鍵と呼ぶ）が格納されており、その鍵と復号器は利用者からも保護されている。ソフト提供者は、ソフトウェアを固有の鍵（ここではソフト鍵と呼ぶ）で暗号化するとともに、用いたソフト鍵を端末鍵で暗号化した鍵データを作成する。販売時には、ユーザーに暗号化されたソフトウェアおよび鍵データを組にして提供する。鍵データはソフト鍵を端末鍵で暗号化したものであるので、特定の計算機においてのみ鍵データを復号してソフト鍵を取得することができる。そして、このソフト鍵を用いて暗号化されたソフトウェアを復号し実行できる。

【0006】2つめの方法は、ソフトウェアの利用に対して課金を行ない、ソフトウェアの配布は無料とするものである。従来からある課金に対する考え方の基本は（流通=課金対象）でありソフトウェアの取得行為に対して課金する方法とみなすことができるが、この方法においては流通は無料にする代りに（利用=課金対象）とする方がディジタル情報提供サービスには適するという考えに基づくものである。この方法の具体例としては、

40 “超流通”と呼ばれる方式がある。なお、超流通は、次の文献に詳しい。

・森亮一、田代秀一：“ソフトウェア・サービス・システム（SSS）の提案”，電子情報通信学会論文誌，Vol. J70D, No. 1, pp. 70-81. . Ryoichi Mori, Masaji Kawahara: “Superdistribution: The Concept and the Architecture”, Trans. of IEICE, Vol. E73, No. 7, pp. 1133-1

超流通の基本コンセプトは、以下の通りである。

(1) 情報利用者は、デジタル情報をほとんど無料で入手できる。すなわち、販売店から購入する以外に、人からコピーをもらう形態も許す。

(2) 情報利用者の端末には、課金管理を行う装置が内蔵されており、情報を実際に利用するごとに課金装置に記録されていく。すなわち、使用量に応じて課金される。

(3) 情報利用者はプリペイド方式あるいはクレジット方式などにより情報の利用可能度数を表すデータ（共通クレジットと呼ばれる）を購入し、その共通クレジットを端末に渡すことによりデジタル情報を利用できる。

【0007】このように利用行為に対して課金できる仕組みを構築することにより、著作権保護を実現するだけでなく、コピーしても元の情報からの劣化が生じないデジタル情報の特徴を積極的に利用することにより流通コストを極端に下げ、実質的なソフト単価を著しく低く抑えることを可能にするのが超流通のねらいである。

【0008】超流通においては、ソフトウェアを利用するごとに課金できるような仕組みをどのように実現するかが最も重要なとなる。具体例としては、配布されるソフトウェアは、ソフトウェア本体とその実行処理に対する課金管理を行うプログラムの2つで構成されており、いずれも暗号化された状態で流通される。ユーザー計算機には課金管理を行うモジュールが存在し、そのモジュールは暗号ソフトの復号を行い、ソフトウェアに添付された課金プログラムを起動する。課金プログラムは配布ソフトの使用状況を監視し、被課金行為が発生するごとに共通クレジットの減額を行う。共通クレジットがある値以上でないとソフトウェアは起動できないようになる。ソフトウェアを再起動するためには、サービスセンタに通信回線によりアクセスし、ある額のクレジット情報を購入する。この課金管理のモジュールは、ユーザーの不正使用から保護されていかなければならない。また、超流通では、コピーそのものを渡すだけで同一の暗号化ソフトがどの端末でも動作することを想定しているため、どの課金モジュールにも共通の暗号鍵が記憶されるものとしている。

【0009】以上のように、従来からソフトウェアに対する著作権保護を可能とする技術が検討されている。しかしながら、このようなソフトウェアに対して考案された著作権保護技術は、そのまま他のデジタル情報に転用することを考えた場合、十分でない面がある。例えば、新聞における記事の切抜きやビデオ映像におけるダビング編集など、いわゆるデジタル情報の2次使用に関する著作権保護や課金の問題である。すなわち、上記超流通は、デジタル情報の2次使用を考慮していないので、2次使用が日常的に行われるであろう現実の情報配布システムに適用することは極めて困難である。もちろん、2次使用を禁止すれば、著作権者の利益は守られ

るが、その一方で利用者の自由を大きく制限することになってしまう。

【0010】また、超流通のように情報の利用と課金を一体化するシステムでは、万一、保護装置が破られた場合に、システム全体に被害が波及するおそれがあるが、この点は保証されていない。

【0011】

【発明が解決しようとする課題】以上説明したように、従来の情報配布システムでは、情報の2次使用に対する

10 著作権保護や課金の技術が十分でなかった。また、情報の利用と課金を一体化するシステムでは、万一、復号鍵等を格納している保護装置が破られた場合にシステム全体に被害が波及するおそれがあった。

【0012】本発明は、上記事情に鑑みてなされたものであり、有料のデジタル情報の配布は供給局から行なうだけでなく、既にそのデジタル情報を取得している端末間での2次配布も可能であり、万一端末装置の物理的安全性が保証されなくなったとしても被害がその端末装置以外に及ばない情報配布システムおよび情報配布方法を提供することを目的とする。また、デジタル情報の配布自体は無償とし、デジタル情報の利用時に課金することのできる情報配布システムおよび情報配布方法を提供することを目的とする。

【0013】

【課題を解決するための手段】上記目的を達成するためには本発明（請求項1）では、デジタル情報の配布を行う情報供給局と、前記デジタル情報を受ける複数の情報端末と、前記情報供給局および前記複数の情報端末の相互間を接続する情報伝達媒体とから構成されるとともに、各情報端末間では前記情報供給局から配布された前記デジタル情報を2次的に配布する情報配布システムにおいて、前記情報供給局は、前記デジタル情報ごとに固有に割り当てた第1の暗号鍵を用いて該デジタル情報を暗号化した暗号化デジタル情報と、この暗号化デジタル情報を伝達すべき前記情報端末に固有に割り当てられた第2の暗号鍵を用いて該第1の暗号鍵に対応する第1の復号鍵を暗号化した暗号化配布鍵とを前記情報伝達媒体に出力する手段を備え、前記情報端末夫々は、前記情報供給局または他の前記情報端末から前記情

30 報伝達媒体を介して伝達された前記暗号化デジタル情報および前記暗号化配布鍵を入力する入力手段と、前記第2の暗号鍵に対応する固有の第2の復号鍵を用いて前記暗号化配布鍵を復号した後、この復号により得られる前記第1の復号鍵を用いて前記暗号化デジタル情報を復号する復号手段と、前記暗号化配布鍵を前記第2の復号鍵を用いて復号した後、この復号により得られる前記第1の復号鍵を、前記暗号化ディジタル情報を伝達すべき別の前記情報端末に固有に割り当てられた前記第2の暗号鍵を用いて暗号化する暗号化配布鍵変換手段と、この暗号化配布鍵変換手段により得られる前記暗号化配布

40 報伝達媒体を介して伝達された前記暗号化ディジタル情報および前記暗号化配布鍵を入力する入力手段と、前記第2の暗号鍵に対応する固有の第2の復号鍵を用いて前記暗号化配布鍵を復号した後、この復号により得られる前記第1の復号鍵を用いて前記暗号化ディジタル情報を復号する復号手段と、前記暗号化配布鍵を前記第2の復号鍵を用いて復号した後、この復号により得られる前記第1の復号鍵を、前記暗号化ディジタル情報を伝達すべき別の前記情報端末に固有に割り当てられた前記第2の暗号鍵を用いて暗号化する暗号化配布鍵変換手段と、この暗号化配布鍵変換手段により得られる前記暗号化配布

50 報伝達媒体を介して伝達された前記暗号化ディジタル情報および前記暗号化配布鍵を入力する入力手段と、前記第2の暗号鍵に対応する固有の第2の復号鍵を用いて前記暗号化配布鍵を復号した後、この復号により得られる前記第1の復号鍵を用いて前記暗号化ディジタル情報を復号する復号手段と、前記暗号化配布鍵を前記第2の復号鍵を用いて復号した後、この復号により得られる前記第1の復号鍵を、前記暗号化ディジタル情報を伝達すべき別の前記情報端末に固有に割り当てられた前記第2の暗号鍵を用いて暗号化する暗号化配布鍵変換手段と、この暗号化配布鍵変換手段により得られる前記暗号化配布

鍵と前記暗号化ディジタル情報を前記情報伝達媒体に出力する出力手段とを備えたことを特徴とする。

【0014】好ましくは、前記情報端末夫々は、前記復号手段により得られる前記暗号化ディジタル情報を編集するための編集手段と、前記暗号化ディジタル情報または前記復号手段により復号されたディジタル情報を利用するごとに更新される利用可能度数情報を格納する利用可能度数情報格納手段と、前記復号手段による前記暗号化ディジタル情報の復号行為および前記編集手段による前記ディジタル情報の編集行為に応じた利用情報の記録を生成するとともに、前記復号行為および前記編集行為に応じて前記利用可能度数情報格納手段に格納された前記利用可能度数情報の更新を行う利用管理手段とをさらに備えることを特徴とする。

【0015】また、好ましくは、前記復号手段および前記暗号化配布鍵変換手段は、外部から物理的に保護された領域に設けられたことを特徴とする。また、本発明

(請求項4)では、デジタル情報を配布を行う情報供給局と、前記デジタル情報を受ける複数の情報端末と、前記情報供給局および前記複数の情報端末の相互間を接続する情報伝達媒体とから構成されるとともに、各情報端末間では前記情報供給局から配布された前記デジタル情報を2次的に配布する情報配布システムにおいて、前記情報供給局は、前記デジタル情報ごとに固有に割り当てた第1の暗号鍵を用いて該デジタル情報を暗号化した暗号化ディジタル情報およびこの暗号化ディジタル情報を伝達すべき前記情報端末に固有に割り当てられた第2の暗号鍵を用いて該第1の暗号鍵に対応する第1の復号鍵を暗号化した暗号化配布鍵、または該暗号化配布鍵のみを前記情報伝達媒体に出力する手段を備え、前記情報端末夫々は、前記情報伝達媒体を介して、前記情報供給局から伝達された前記暗号化ディジタル情報および前記暗号化配布鍵または、他の前記情報端末から伝達された前記暗号化ディジタル情報および前記情報供給局から伝達された前記暗号化配布鍵を入力する入力手段と、前記第2の暗号鍵に対応する固有の第2の復号鍵を用いて前記暗号化配布鍵を復号した後、この復号により得られる前記第1の復号鍵を用いて前記暗号化ディジタル情報を復号する復号手段と、前記暗号化ディジタル情報を前記情報伝達媒体に出力する出力手段とを備えたことを特徴とする。

【0016】好ましくは、前記情報供給局は、前記情報端末夫々に対する前記暗号化配布鍵の配布行為を記録する手段をさらに備え、前記情報端末夫々は、前記復号手段により得られる前記暗号化ディジタル情報を編集するための編集手段と、前記暗号化ディジタル情報または前記復号手段により復号されたディジタル情報を利用するごとに更新される利用可能度数情報を格納する利用可能度数情報格納手段と、前記復号手段による前記暗号化ディジタル情報の復号行為および前記編集手段による前記

デジタル情報の編集行為に応じた利用情報の記録を生成するとともに、前記復号行為および前記編集行為に応じて前記利用可能度数情報格納手段に格納された前記利用可能度数情報の更新を行う利用管理手段とをさらに備えることを特徴とする。

【0017】また、好ましくは、前記復号手段は、外部から物理的に保護された領域に設けられた特徴とする。

一方、本発明(請求項7)では、第1の情報端末が、デジタル情報を配布を受けるとともに、受けたデジタル情報を第2の情報端末に2次的に配布する情報配布方法において、前記デジタル情報ごとに固有に割り当てた第1の暗号鍵を用いて該デジタル情報を暗号化した暗号化ディジタル情報と、前記第1の情報端末に固有に割り当てられた第2の暗号鍵を用いて該第1の暗号鍵に対応する第1の復号鍵を暗号化した暗号化配布鍵とを入力する入力ステップと、前記第2の暗号鍵に対応する固有の第2の復号鍵を用いて前記暗号化配布鍵を復号する復号ステップと、この復号ステップにより得られる前記第1の復号鍵を、前記第2の情報端末に固有に割り当てられた前記第2の暗号鍵を用いて暗号化する暗号化ステップと、この暗号化ステップにて得られる前記暗号化配布鍵と前記暗号化ディジタル情報を出力する出力ステップとを有することを特徴とする。

【0018】また、本発明(請求項8)では、第1の情報端末が、デジタル情報を配布を受けるとともに、受けたデジタル情報を第2の情報端末に2次的に配布する情報配布方法において、前記デジタル情報ごとに固有に割り当てた第1の暗号鍵を用いて該デジタル情報を暗号化した暗号化ディジタル情報および前記第1の情報端末に固有に割り当てられた第2の暗号鍵を用いて該第1の暗号鍵に対応する第1の復号鍵を暗号化した暗号化配布鍵を入力する入力ステップと、前記第2の暗号鍵に対応する固有の第2の復号鍵を用いて前記暗号化配布鍵を復号する復号ステップと、この復号ステップにより得られる前記第1の復号鍵を、前記第2の情報端末に固有に割り当てられた前記第2の暗号鍵を用いて暗号化する暗号化ステップと、この暗号化ステップにて得られる前記暗号化配布鍵と前記暗号化ディジタル情報を出力する出力ステップとを有することを特徴とする。

【0019】

【作用】請求項1の発明では、配布するデジタル情報には固有に第1の暗号鍵・第1の復号鍵を割り当て、各情報端末には固有に公開鍵暗号方式による第2の暗号鍵・

第2の復号鍵を固有に割り当てる。なお、第1の暗号鍵・第1の復号鍵は、公開鍵暗号方式および慣用暗号方式のいずれを利用してても良く、慣用暗号方式による場合は2つの鍵は同一のものとなる。

【0020】情報供給局では、デジタル情報を固有の第1の暗号鍵で暗号化して暗号化ディジタル情報を生成し、これを受信情報端末へ配布するとともに、受信情報端末が暗号化ディジタル情報を復号する際に必要な第1の復号鍵を上記したような受信端末固有の第2の暗号鍵で暗号化した暗号化配布鍵を配送する。

【0021】また、既に暗号化ディジタル情報の配布を受けた情報端末から他の情報端末へは、暗号化ディジタル情報をそのまま配布するとともに、情報供給局から得た当該情報端末用に暗号化された暗号化配布鍵を他の情報端末用に暗号化しなおして伝える。

【0022】受信端末は、暗号化された第1の復号鍵を該端末に固有の第2の復号鍵で復号して該第1の復号鍵を取出した後、この第1の復号鍵を用いて暗号化されたディジタル情報を復号する。

【0023】ここで、本発明では、暗号化ディジタル情報を基本的には制限なく配布し得る一方、該暗号化ディジタル情報の暗号化に用いた第1の暗号鍵に対応する第1の復号鍵を自端末に固有の第2の暗号鍵で暗号化した暗号化配布鍵を獲得した情報端末のみが、暗号化ディジタル情報を復号することが可能である。

【0024】従って、著作権を保護しつつ、ディジタル情報の配布を情報供給局から行なうばかりでなく、既に情報供給局から配布を受けている情報端末からそうでない情報端末へも2次的に配布することが可能である。

【0025】また、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその情報端末以外に及ばず、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。すなわち、本発明では、個々の情報端末ごとに固有に割当てられた暗号鍵が内蔵されている。このため、ある端末が破られて内蔵されていた暗号鍵が外部に知られたとしても、特定の端末の複製品だけが複数存在する状況になる。従って、破られた特定の端末向けに配布した情報に対しては正当に課金されないが、それ以外の情報に対する課金は正常に機能する。さらに、そのような状態では破られた鍵が特定された場合にその鍵を使用不能にする必要があるが、破られた鍵から端末が特定でき、その端末の鍵を更新するだけでよい。これに対し、従来のようにすべての情報端末に同一の暗号鍵が内蔵されている場合には全端末の暗号鍵を更新する必要が生じるが、それは極めて困難である。

【0026】また、例えば請求項2の発明のように情報端末内に課金管理を行う装置を内蔵し、その装置により利用状態を管理すれば、配布情報の切り出しや複写などの編集行為に対しても課金を正常に行うことができる。

【0027】また、請求項4の発明では、配布するディジタル情報には固有に第1の暗号鍵・第1の復号鍵を割当て、各情報端末には固有に第2の暗号鍵・第2の復号鍵を固有に割当てる。なお、第1の暗号鍵・第1の復号鍵は、公開鍵暗号方式および慣用暗号方式のいずれを利用しても良く、慣用暗号方式による場合は2つの鍵は同一のものとなる。また、第2の暗号鍵・第2の復号鍵は、慣用暗号方式による場合は同一のものとなる。

【0028】情報供給局では、ディジタル情報は固有の第1の暗号鍵で暗号化して暗号化ディジタル情報を生成し、これを受信情報端末へ配布するとともに、受信情報

端末が暗号化ディジタル情報を復号する際に必要な第1の復号鍵を上記したような受信端末固有の第2の暗号鍵で暗号化した暗号化配布鍵を配信する。

【0029】また、既に暗号化ディジタル情報の配布を受けた情報端末から他の情報端末へは、暗号化ディジタル情報をそのまま配布する。この場合、請求項1の発明と異なる点は、他の情報端末に対して、必ず、情報供給局から受信情報端末用の暗号化配布鍵を配信する点である。

10 【0030】受信端末は、暗号化された第1の復号鍵を該端末に固有の第2の復号鍵で復号して該第1の復号鍵を取出した後、この第1の復号鍵を用いて暗号化されたディジタル情報を復号する。

【0031】ここで、本発明では、暗号化ディジタル情報を基本的には制限なく配布し得る一方、該暗号化ディジタル情報の暗号化に用いた第1の暗号鍵に対応する第1の復号鍵を自端末に固有の第2の暗号鍵で暗号化した暗号化配布鍵を獲得した情報端末のみが、暗号化ディジタル情報を復号することが可能である。

20 【0032】従って、著作権を保護しつつ、ディジタル情報の配布を情報供給局から行なうばかりでなく、既に情報供給局から配布を受けている情報端末からそうでない情報端末へも2次的に配布することが可能である。

【0033】また、請求項1の発明と同様に、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその情報端末以外に及ばず、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。

30 【0034】また、例えば請求項5の発明のように情報端末内に課金管理を行う装置を内蔵し、その装置により利用状態を管理するために、配布情報の切り出しや複写などの編集行為に対しても課金を正常に行うことができる。

【0035】また、本発明によれば、配布された情報を復号するためには情報供給局にアクセスする必要があり、そのアクセス行為を記録することにより情報供給局で課金管理をすることが可能となる。

【0036】一方、請求項7の発明では、配布されるディジタル情報には固有に第1の暗号鍵・第1の復号鍵が割当てられ、情報端末には固有に公開鍵暗号方式による第2の暗号鍵・第2の復号鍵が固有に割当てる。なお、第1の暗号鍵・第1の復号鍵は、公開鍵暗号方式および慣用暗号方式のいずれを利用しても良く、慣用暗号方式による場合は2つの鍵は同一のものとなる。

【0037】情報端末には、ディジタル情報は固有の第1の暗号鍵で暗号化した暗号化ディジタル情報と、この暗号化ディジタル情報を復号する際に必要な第1の復号鍵を上記したような当該端末固有の第2の暗号鍵で暗号化した暗号化配布鍵が配布される。

50 【0038】また、この情報端末は、既に暗号化ディジタル情報の配布を受けている場合、他の情報端末へ、当

該暗号化ディジタル情報をそのまま配布するとともに、既に獲得してある当該情報端末用に暗号化された暗号化配布鍵を他の情報端末用に暗号化しなおして伝えることができる。

【0039】情報端末は、暗号化された第1の復号鍵を該端末に固有の第2の復号鍵で復号して該第1の復号鍵を取出した後、この第1の復号鍵を用いて暗号化されたディジタル情報を復号することができる。

【0040】ここで、本発明では、暗号化ディジタル情報を基本的には制限なく配布し得る一方、該暗号化ディジタル情報の暗号化に用いた第1の暗号鍵に対応する第1の復号鍵を自端末に固有の第2の暗号鍵で暗号化した暗号化配布鍵を獲得した情報端末のみが、暗号化ディジタル情報を復号することが可能である。

【0041】従って、著作権を保護しつつ、情報端末は、ディジタル情報の配布を受けることができるばかりでなく、既に配布を受けている場合、他の情報端末へも当該ディジタル情報を2次的に配布することが可能である。

【0042】また、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその情報端末以外に及ぼす、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。

【0043】また、請求項8の発明では、配布されるディジタル情報には固有に第1の暗号鍵・第1の復号鍵が割当てられ、各情報端末には固有に第2の暗号鍵・第2の復号鍵が固有に割当てられる。なお、第1の暗号鍵・第1の復号鍵は、公開鍵暗号方式および慣用暗号方式のいずれを利用しても良く、慣用暗号方式による場合は2つの鍵は同一のものとなる。また、第2の暗号鍵・第2の復号鍵は、慣用暗号方式による場合は同一のものとなる。

【0044】情報端末には、ディジタル情報は固有の第1の暗号鍵で暗号化した暗号化ディジタル情報と、この暗号化ディジタル情報を復号する際に必要な第1の復号鍵を上記したような当該端末固有の第2の暗号鍵で暗号化した暗号化配布鍵が配布される。

【0045】また、既に暗号化ディジタル情報の配布を受けた情報端末から他の情報端末へは、暗号化ディジタル情報をそのまま配布することができる。受信端末は、暗号化された第1の復号鍵を該端末に固有の第2の復号鍵で復号して該第1の復号鍵を取出した後、この第1の復号鍵を用いて暗号化されたディジタル情報を復号する。

【0046】ここで、本発明では、暗号化ディジタル情報を基本的には制限なく配布し得る一方、該暗号化ディジタル情報の暗号化に用いた第1の暗号鍵に対応する第1の復号鍵を自端末に固有の第2の暗号鍵で暗号化した暗号化配布鍵を獲得した情報端末のみが、暗号化ディジタル情報を復号することができる。

【0047】従って、著作権を保護しつつ、情報端末は、ディジタル情報の配布を受けることができるばかりでなく、既に情報供給局から配布を受けている情報端末からそうでない情報端末へも2次的に配布することが可能である。

【0048】また、請求項1の発明と同様に、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその情報端末以外に及ぼす、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。

10 【0049】

【実施例】以下、図面を参照しながら本発明の実施例を説明する。図1には、本発明の一実施例に係る情報配布システムの構成を示す。この情報配布システムは、利用者に情報を無償で配布し、情報の利用時に初めて課金を行うような情報配布形態を実現しようとする場合に好適であり、情報配布サービスを提供する情報供給局101、情報の伝達に供される通信システム（情報伝達媒体）102、情報の配布を受けるとともに、受けた情報をそのままあるいは加工して2次的に配布することができる情報端末103、および後述するように本システムで用いられる暗号鍵の管理などをするサービスセンタ104からなる。

【0050】本実施例で扱う配布情報は、デジタル化されたテキスト・音声・画像あるいはこれらが混在した形式であり、例えば、新聞、雑誌などの出版物に代表される文書（および静止画）情報や、音楽、映画などの視聴覚的な情報を含むものとする。

【0051】情報供給局101は、情報端末103の要求等に応じて、有料の情報（特に著作物）の配布を行う。当該情報配布システム内に設ける情報供給局101の数は任意である。

【0052】情報端末103は、情報供給局101から情報の配布を受ける機能、配布された情報を表示する機能の他に、情報を編集するための機能、他の情報端末との通信機能などを有する。そして、必要に応じ、受け取った情報をそのままあるいは加工して他の情報端末103に渡すことができる。情報端末103の数は任意である。

【0053】サービスセンタ104は、個々の情報端末103の暗号鍵のデータベースを管理しており、必要に応じて情報供給局101もしくは情報端末103からアクセスされる。

【0054】各局101、103、104間での情報の伝達は通信システム102を介して行われる。なお、デジタル化された有料情報の配布や後述する必要な復号鍵等の伝達にはどのような形態のメディアを利用しても良く、通常の通信回線の他に、放送や記録媒体（例えばCD-R ROMやフロッピーディスク、メモリカードなど）を利用することも可能である。また、例えば有料情報と必要な復号鍵とで互いに異なる情報伝達媒体を利用して

するように構成することも可能である。本実施例では、通信システム102として、通常の通信回線を利用するこことする。

【0055】本実施例では、通信回線等における配布途上データの不正取得や改ざんの保護を実現するために、有料情報は暗号化された状態で配布する。情報供給局101は、配布情報ごとに異なる暗号鍵および復号鍵（以下、配布鍵と呼ぶ）の組（ただし、暗号鍵と復号鍵が同一の場合もある）を設定し、配布情報を暗号鍵で暗号化しておく。情報端末103は復号機能を実装しており、配布鍵を取得すれば暗号化された配布情報を復号することができます。

【0056】また、本実施例では、デジタル情報の特徴を生かした利用形態をユーザに提供するために、情報のコピーは自由（無料）とし、表示や視聴などの行為を有料とする。また、配布された有料情報の全部または一部を編集する行為（例えば情報の一部を切り出し他のデータと合成するような行為；以下、情報の2次使用と呼ぶ）は禁止せずに認めることとし、その代りに情報の2次使用に対して課金をする。

【0057】ここで、情報の配布自体に課金する代りに情報の利用行為に対して課金を行うためには、情報の利用を判別しその結果に応じて課金する機構が必要となる。まず、課金機構を実現する方法としては、例えば次の2つの方法が考えられる。

【0058】1つの方法は、情報供給局101が配布鍵を特定の情報端末103向けに配布する行為を監視し、この行為の記録を取るものである。他の方法は、各情報端末104夫々に、情報の復号行為、情報の編集行為を検出する機構およびユーザの情報利用量を制御する機構（以下、課金モジュールと呼ぶ）を装備するものである。

【0059】前者の方法は、情報供給局101からの有料情報の配布行為に対しては課金が行えるが、それ以外の行為（例えば情報端末103同士での有料情報の配布や情報の2次使用）は課金できないのに対し、後者の方は、情報の配布自体を無料とし、情報を利用した時点で課金することができる。

【0060】本実施例では、情報利用行為自体に対して課金を行うことのできる後者の方法を用いる。なお、後者の方法は、課金モジュールが正常に動作する限りにおいては情報利用量を制御できるが、そのためには課金モジュール自体を攻撃から守る必要があるとともに、加えて著作物単位の使用量を情報提供側が把握するために、課金モジュール内の利用記録を回収する手段が必要となる。これらの点に関し、本実施例では、“超流通システム”にて示されている課金モジュールの構成と利用記録の回収法を適用することができる。簡単に説明すると、次のような仕組みである。ユーザが有料情報を利用するたびに減額される利用可能度数情報（プリペイドカード

に記録されているデータやクレジットに相当する）が存在し、これがユーザからは操作不可能な媒体（例えばICカード）に記録されている。媒体内の利用可能度数情報が不足すると課金モジュールの制御により、配布情報の復号などが実行できなくなる。ユーザがその媒体を情報提供側（本実施例では情報供給局101）に返送すれば、情報提供側が利用可能度数を増やしてこれを再びユーザに配送する。この媒体内に著作物単位の利用記録を課金モジュールの操作により書き込むことにより、情報

10 提供側で度数情報の更新とともに利用記録を回収できる。また、通信回線により利用記録を送信することもできる。通信回線による形態では、情報提供側から受け取り信号を受信しない限りは課金モジュールの制御により情報の利用が不可能となるように構成する。

【0061】次に、以上説明した機能を実現する情報端末103の構成例を図2を参照しながら説明する。図2に示すように、情報端末103は、課金モジュール201、ユーザメモリ202、表示部203、コマンド入力部204、2次記憶インタフェース部205、利用度数記憶媒体インタフェース部206、通信部207を備えている。

【0062】このうち課金モジュール201は、物理的に保護されたモジュールであり、その内部には図3に示すように実行制御部301、暗号器／復号器302、鍵記憶部303、課金管理部304、保護メモリ305が設けられている。課金モジュールを物理的に保護する方法には様々なレベルが存在するが、幾つか例を挙げると、モジュール全体を1チップLSIにより構成する方法、入出力線以外のモジュール全体を樹脂で封止する方法、モジュールに物理的な不正アクセス検出機構を設ける方法、さらに不正アクセスを検出した場合にはモジュール内のメモリ内容等を消去するなどの方法がある。なお、物理的な不正アクセスとは入出力線以外の部分を直接プローピングする行為を想定しており、その具体的な検出機構は例えば、文献 Ryoichi Mori, Masaji Kawahara: “Superdistribution: The Concept and the Architecture”, Trans. of IEICE, Vol. E73, No. 7, pp. 1133-1146に述べられている。

【0063】課金モジュール201は、暗号化された情報を復号する機能、復号した情報を暗号化する機能、および復号した情報を編集するための機能を有し、情報の利用（復号・表示や編集）に対して課金をするとともに、課金できないときは情報の利用を禁止する制御を行う。なお、基本的には、復号された配布情報（平文）は課金モジュール201内部の保護メモリ305に保持され、外部から直接読み出すことはできない。ただし、後述するように、情報の2次利用がされる場合は、課金した後に復号された配布情報（平文）の一部を当該課金モジュール201の外部に出力する。

50 【0064】ユーザメモリ202は、暗号化された情報

等を格納するためのものである。コマンド入力部204は、ユーザからのコマンドを受け付けるためのものであり、入力装置としては例えばキーボードおよび／またはいわゆるマウス等を利用することができます。情報端末103で用いられるコマンドには、配布情報の復号表示、(情報供給局101への)配布情報の要求、(他端末103への)情報の送信、(他端末103からの)情報の受信、情報の編集(2次使用)などが用意される。

【0065】表示部203は、復号された配布情報等を画面表示したり、各コマンドに対応した画面、例えば編集画面や通信画面を表示したりする。利用度数記憶媒体インターフェース部206は、利用度数を記録するための利用度数記憶媒体208を収容するインターフェースである。利用度数記憶媒体208には、例えばICカードを用いると好ましく、この場合、利用度数記憶媒体インターフェース部206には、ICカードリーダを用いることができる。

【0066】通信部207は、配布情報等の送受信を外部と行うための通信インターフェースである。すなわち、各情報端末103は、この通信部207を介して通信システム102に接続されている。

【0067】2次記憶インターフェース部205は、配布された情報を記憶するための2次記憶(図示せず)を収容するインターフェースである。2次記憶には、情報を大量に記憶できるハードディスクやフロッピーディスクなどを用いると好ましい。

【0068】以下、上記構成における動作例を概略的に説明する。前述したように配布された有料情報は暗号化されている。情報端末103では、配布情報の復号表示コマンドを受け付けると、情報の復号を行う前に、まず課金モジュール201内の課金管理部304が利用度数記憶媒体208内の残高度数を調べる。残高度数が復号表示に必要な度数以上であれば、実行制御部301に“実行可能信号”を送る。これを受けて実行制御部301は2次記憶(図示せず)もしくはユーザメモリ202から配布情報を課金モジュール201内の保護メモリ305に転送する。

【0069】なお、配布情報が大量の場合には、実際に表示される領域の周辺だけを転送するようにしても良い。例えば、雑誌などの情報であれば表示部203で表示可能な頁サイズのデータだけを転送し、ユーザからの貢めくりコマンドの入力の度に対応するデータを転送するようにすると、処理が高速化できるので効果的である。

【0070】実行制御部301は、課金モジュール201内の情報を鍵記憶部303に格納している復号鍵を用い暗号器/復号器302の暗号機能により復号し、保護メモリ305に格納する。表示部203では保護メモリ305の内容にアクセスし、画面表示などを行う。

【0071】課金モジュール201では、課金管理部3

04にて、例えば復号表示した頁数をカウントし、その都度、頁あたりの表示分の度数を度数記憶媒体208内の度数情報から減額する。度数記憶媒体208が外されている場合など、減額に成功しないときには課金モジュール201内の実行制御モジュール301が保護メモリ305の内容をクリアするなどの処理を行って、配布情報が利用できないようとする。

【0072】ここで、情報端末103では情報の2次使用を行うことができる。この情報の2次使用としては、

10 表示されている情報に対する切り抜き行為が典型的である。この場合、例えば範囲指定/ファイルへの保存をユーザコマンドとして実行することになる。そして、課金モジュール201は範囲指定コマンドからその領域の切り抜きに対する課金額を計算し、度数情報を参照し、減額可能であれば実行し、そうでない場合にはエラーメッセージを表示して実行しないようとする。課金額の計算に必要な料金情報は、配布物ごとに添付されており、“頁あたりの表示料金”、頁あたりの切り抜き料金などのデータを含んでいる。

20 【0073】なお、配布物について2次使用を許可/禁止することを示す情報を付加し、この情報に従って、2次使用を許可/禁止するように構成することも可能である。2次使用が禁止されている場合、復号された配布情報(平文)が課金モジュール201の外部へ出力されることはない。

【0074】以上が、情報端末103の構成および機能である。次に、上述した構成を有する情報配布システムにおいて用いる情報配布(1次配布および2次配布)の方式を2種類のものについて説明する。

30 【0075】図4は第1の情報配布方式を示しており、情報の配達に慣用暗号方式を、配布鍵の転送に公開鍵暗号方式を利用した構成である。各情報端末103の課金モジュール201内部の鍵記憶部303には、それぞれ固有の秘密鍵(復号鍵)が記憶されている。一方、公開鍵(暗号鍵)は情報供給局101および各情報端末103からアクセス可能な状態で公開されている。以下、本方式の説明では、情報供給局101から情報の配布を受けようとする情報端末#iの秘密鍵をSK_iとし、公開鍵をPK_iとする。

40 【0076】公開鍵の管理は、図1のサービスセンタ104内に公開データベースを設置することで行っても良いし、あるいは、公開鍵と情報端末#iのID情報を組にして織り込んだデータにサービスセンタ104がデジタル署名を行った“公開鍵証明書”を情報端末#iが保有し、要求の都度公開鍵証明書を交換することで行ってもよい。

【0077】情報供給局101では、情報Pごとに固有の“配布鍵WK_P”を定め、情報を配布鍵により暗号化する。このときの暗号方式には、処理速度が高速な慣用暗号を利用する。この暗号化配布情報を、C_P=W

K__P (P) と記述することにする。情報端末# i は、配布鍵WK__Pを得ることにより、暗号化配布情報を基にして通常の配布情報を復元することが可能である。

【0078】以下、図5のフローチャートを参照しながら、情報供給局101から情報端末# iへの情報の1次配布の手順を説明する。なお、情報供給局101では、既に、情報Pを固有の配布鍵WK__Pで暗号化し、暗号化配布情報C__Pおよび配布鍵WK__Pをリンクして図示しない記憶装置に格納してあるものとする。

【0079】最初に情報端末# i から情報供給局101へ情報Pの配布の要求が発生する(ステップS1)。情報供給局101は要求元の情報端末# i に対応する公開鍵PK__i をサービスセンタ104から取得する(ステップS2)。

【0080】情報供給局101と情報端末# i の間で認証プロトコルを実行し、情報供給局101は情報端末# i の正当性を確認する(ステップS3)。ここで認証プロトコルは、相手端末が秘密鍵SK__i を所持している事実を確認するものであり、例えば検査側(ここでは情報供給局101)から乱数を送り、被認証側(ここでは情報端末# i)がその乱数を秘密鍵SK__i で暗号化して返送し、検査側では公開鍵PK__i で逆変換して送信した乱数が現れることを検査すればよい。

【0081】認証に成功した場合(ステップS4でYe sの場合)、情報供給局101は、暗号化情報C__Pに用いた配布鍵WK__Pを記憶装置から検索し(ステップS6)、この配布鍵WK__Pを情報端末# i の公開鍵で暗号化する(ステップS7)。このようにして生成される情報を暗号化配布鍵と呼ぶことになるとともに、D__i P = PK__i (WK__P) と表記することにする。

【0082】次に、配布する情報Pの暗号化情報C__Pを検索し(ステップS8)、暗号化配布情報C__Pおよび暗号化配布鍵D__i Pを情報端末# i に配布する(ステップS9)。

【0083】上記1次配布により暗号化配布情報C__Pおよび暗号化配布鍵D__i Pを受信した情報端末# i は、課金モジュール201内の鍵記憶部303に格納してある秘密鍵SK__i を用い暗号器/復号器302の復号機能により暗号化配布鍵D__i Pから配布鍵WK__Pを取り出し、さらに配布鍵WK__Pで暗号化配布情報C__Pを復号することができる。配布鍵WK__Pは情報端末# i の課金モジュール201外部には現れず、配布情報の保存時には、暗号化配布情報C__Pとその暗号化配布鍵D__i Pがリンク付けされ格納される。

【0084】なお、ステップS1で、情報端末# i から情報供給局101へ情報Pの配布を要求することで情報配布を開始する代わりに、情報供給局101から情報端末# i へ情報Pの配布を通知することで情報配布を開始することも可能である。

【0085】次に、図6のフローチャートを参照しなが

ら、情報端末# i から情報端末# j への情報の2次配布の手順を説明する。なお、情報端末# i は、既に、情報供給局101から配布情報Pに対応する暗号化配布情報C__Pを入手しており、暗号化配布情報C__Pとその暗号化配布鍵D__i Pをリンク付けし格納してあるものとする。

【0086】情報供給局101からの1次配布の場合と同様に、最初に情報端末# j から情報端末# i へ情報Pの配布の要求が発生する(ステップS11)。情報端末# i は要求元の情報端末# j に対応する公開鍵PK__j をサービスセンタ104から取得する(ステップS12)。

【0087】次に、1次配布の場合と同様の方法で、情報端末# i 、 j の間で認証プロトコルを実行する(ステップS13)。なお、このステップS13の認証プロトコルの実行は省いても構わない。

【0088】認証に成功した場合(ステップS14でYe sの場合)、情報端末# i は暗号化配布鍵D__i Pを検索する(ステップS16)。次に、検索した暗号化配布鍵D__i Pを基にして情報端末# j に渡す暗号化配布鍵D__j Pを生成する(ステップS17)。まず、情報端末# i は暗号化配布鍵D__i Pと情報端末# j の公開鍵PK__j を課金モジュール201に入力する。課金モジュール201では、情報端末# i 用の暗号化配布鍵D__i Pから配布鍵WK__Pを取り出し、さらに情報端末# j に対応する公開鍵PK__j で暗号化した情報端末# j 用の暗号化配布鍵D__j P = PK__j (WK__P) を生成する。

【0089】次に、配布する情報Pの暗号化情報C__Pを検索し(ステップS18)、暗号化配布情報C__Pおよび暗号化配布鍵D__j Pを、情報端末# j に配布する(ステップS19)。

【0090】上記2次配布により暗号化配布情報C__Pおよび暗号化配布鍵D__j Pを受信したを受信した情報端末# j は、課金モジュール201内の鍵記憶部303に格納してある秘密鍵SK__j を用い暗号器/復号器302の復号機能により暗号化配布鍵D__j Pから配布鍵WK__Pを取り出し、さらに配布鍵WK__Pで暗号化配布情報C__Pを復号することができる。配布鍵WK__Pは情報端末# j の課金モジュール201外部には現れず、配布情報の保存時には、暗号化配布情報C__Pとその暗号化配布鍵D__j Pがリンク付けされ格納される。

【0091】なお、ステップS11で、情報端末# j から情報端末# i へ情報Pの配布を要求することで情報配布を開始する代わりに、情報端末# i から情報端末# j へ情報Pの配布を通知することで情報配布を開始することも可能である。

【0092】本方式では、暗号化配布鍵D__i PからD__j Pの作成のような暗号化配布鍵の変換処理は、2次配布の度に必要となるが、暗号化配布情報C__P自体は

そのまま配布できる。通常、情報Pのサイズは配布鍵WK_Pに比べ極めて大きいため、暗号化配布情報C_Pを再暗号化することなく利用できるのは有効である。

【0093】なお、公開鍵暗号としてRSA(Rivest-Shamir-Adleman)暗号を用いた場合、同じWK_Pを複数の暗号鍵で暗号化することになるが、このような場合には攻撃法の存在が知られている。攻撃法の具体例は次の文献に詳しい。

J. Hastad, "On using RSA with low exponent in a public key network", Lecture Notes in Computer Science: Advances in Cryptology - CRYPTO'85 proceedings, Springer-Verlag, pp. 403-408.

そこで、公開鍵暗号としてRSA暗号を用いる場合は、RSAの1ブロックとして暗号化できる平文のサイズは慣用暗号による配布鍵のサイズよりも大きいため、例えば配布セッションごとに異なる乱数Rを生成し、 $R \parallel WK_P$ (但し、 \parallel はデータの連結を意味する)を暗号化配布鍵の平文として用いるなどすれば好ましい。

【0094】次に、第2の情報配布方式について説明する。図7は、第2の情報配布方式を示しており、情報の配送および配布鍵の転送とともに、慣用暗号方式を利用した構成である。ただし、第1の情報配布方式のように、配布鍵の転送に公開鍵暗号方式を利用しても構わない。

【0095】各情報端末103には、課金モジュール201内部の鍵記憶部303に固有の秘密鍵が記憶されている。この場合には、慣用暗号のため、秘密鍵は暗号化と復号化の両方に用いられる。以下、本方式の説明では、情報端末#iの秘密鍵をK_iとする。

【0096】秘密鍵K_iのデータベースはサービスセンタ104が管理しており、個々の情報端末103に対応する秘密鍵K_iはサービスセンタ104のみが把握可能である。情報供給局101はサービスセンタ104にアクセスし、秘密鍵情報を取得できる。ただし、本実施例では、情報端末103からは秘密鍵情報を取得できないものとする。

【0097】情報供給局101では、情報Pごとに固有の“配布鍵WK_P”を定め、情報を配布鍵により暗号化する。このときの暗号方式には、処理速度が高速な慣用暗号を利用する。この暗号化情報を、 $C_P = WK_P (P)$ と記述することにする。情報端末#jは、配布鍵WK_Pを得ることにより、暗号化配布情報を基にして通常の配布情報を復元することが可能である。

【0098】以下、図8のフローチャートを参照しながら、情報供給局101から情報端末#iへの情報の1次配布の手順を説明する。なお、情報供給局101では、既に、情報Pを固有の配布鍵WK_Pで暗号化し、情報

P、暗号化配布情報C_Pおよび配布鍵WK_Pをリンクして図示しない記憶装置に格納してあるものとする。

【0099】最初に情報端末#iから情報供給局101へ情報Pの配布の要求が発生する(ステップS21)。情報供給局101は要求元の情報端末#iに対応する公開鍵K_iをサービスセンタ104から取得する(ステップS22)。

【0100】情報供給局101は情報端末#iとの間で認証プロトコルを実行し、情報端末#iの正当性を確認

10 する(ステップS23)。ここで認証プロトコルは、相手端末が確かに秘密鍵K_iを所持している事実を確認するものであり、例えば検査側(ここでは情報供給局101)から乱数を送り、被認証側(ここでは情報端末#i)がその乱数を秘密鍵K_iで暗号化して返送し、検査側では端末#iの鍵K_iで逆変換して送信した乱数が現れることを検査すればよい。

【0101】認証に成功した場合(ステップS24でYESの場合)、情報供給局101は、暗号化情報C_P

20 に用いた配布鍵WK_Pを記憶装置から検索し(ステップS26)、この配布鍵WK_Pを情報端末#iの秘密鍵で暗号化する(ステップS27)。このようにして生成される情報を暗号化配布鍵と呼ぶことになるとともに、 $D_i P = K_i (WK_P)$ と表記することにする。

【0102】次に、配布する情報Pの暗号化情報C_Pを検索し(ステップS28)、暗号化配布情報C_Pおよび暗号化配布鍵D_i Pを情報端末#iに配布する(ステップS29)。

【0103】上記1次配布により暗号化配布情報C_Pおよび暗号化配布鍵D_i Pを受信した情報端末#iは、課金モジュール201内の鍵記憶部303に格納してある秘密鍵K_iを用い暗号器/復号器302の復号機能により暗号化配布鍵D_i Pから配布鍵WK_Pを取り出し、さらに配布鍵WK_Pで暗号化配布情報C_Pを復号する。配布鍵WK_Pは情報端末#iの課金モジュール201外部には現れず、配布情報の保存時には、暗号化配布情報C_Pとその暗号化配布鍵D_i Pがリンク付けされ格納される。

【0104】なお、ステップS21で、情報端末#iから情報供給局101へ情報Pの配布を要求することで情報配布を開始する代わりに、情報供給局101から情報端末#iへ情報Pの配布を通知することで情報配布を開始することも可能である。

【0105】次に、図9のフローチャートを参照しながら、情報端末#iから情報端末#jへの情報の2次配布の手順を説明する。なお、情報端末#iは、既に、情報供給局101から配布情報Pに対応する暗号化配布情報C_Pを入手しており、暗号化配布情報C_Pとその暗号化配布鍵D_i Pをリンク付けし格納してあるものとする。

【0106】情報供給局101からの1次配布の場合と同様に、情報端末#jから情報端末#iへ情報Pの配布の要求が発生する（ステップS31）。情報端末#iは、情報Pの暗号化配布情報C_Pを検索し（ステップS32）、情報端末#jへを送信する（ステップS33）。なお、情報端末#iから情報端末#jに暗号化配布情報C_Pを配布するにあたって、情報端末#iは情報端末#jとの間で認証プロトコルは実行しない。

【0107】次に、情報端末#jは暗号化配布情報C_Pの復号に必要な暗号化配布鍵D_j Pを情報供給局101に要求する（ステップS34）。情報供給局101はこの要求に応じてサービスセンタ104から情報端末#jの秘密鍵K_jを取得する（ステップS35）。

【0108】次に、1次配布の場合と同様の方法で、情報供給局101は情報端末#jとの間で認証プロトコルを実行し、情報端末#jの正当性を確認する（ステップS36）。なお、このステップS36は、後述する情報供給局101から暗号化配布鍵を配布した時点で情報端末#jに課金するような方法をとる場合は、暗号化配布鍵の配布先が確実に情報端末#jであるかどうかを確認できるので有効である。また、後述する情報の利用時に初めて課金するような方法をとる場合は、この認証プロトコルの実行は省いても構わない。

【0109】認証に成功した場合（ステップS37でYesの場合）、情報供給局101は、暗号化情報C_Pに用いた配布鍵WK_Pを検索し（ステップS39）、この配布鍵WK_Pを情報端末#jの秘密鍵で暗号化して暗号化配布鍵D_j Pを生成する（ステップS40）。なお、暗号化配布鍵はD_j P = K_j (WK_P)と表記する。

【0110】次に、暗号化配布鍵D_j Pを情報端末#jに配布する（ステップS41）。上記2次配布により暗号化配布情報C_Pおよび暗号化配布鍵D_j Pを受信した情報端末#jは、課金モジュール201内の鍵記憶部303に格納してある秘密鍵K_jを用い暗号器／復号器302の復号機能により暗号化配布鍵D_j Pから配布鍵WK_Pを取り出し、さらに配布鍵WK_Pで暗号化配布情報C_Pを復号することができる。配布鍵WK_Pは情報端末#jの課金モジュール201外部には現れず、配布情報の保存時には、暗号化配布情報C_Pとその暗号化配布鍵D_j Pはリンク付けされ格納される。

【0111】なお、ステップS31で、情報端末#jから情報端末#iへ情報Pの配布を要求することで情報配布を開始する代わりに、情報端末#iから情報端末#jへ情報Pの配布を通知することで情報配布を開始することも可能である。

【0112】この方式では暗号化配布情報C_Pだけが2次配布可能であるので、2次配布情報だけでは情報の利用ができないのが欠点であるが、大量の情報である暗

号化配布情報C_Pは2次配布できる。

【0113】なお、上記各情報配布方式では、2次配布において、配布する情報Pに対応する暗号化情報C_Pは情報端末103のユーザメモリ202や図示しない2次記憶等に格納されており、情報端末103は、暗号化情報C_Pを検索して（ステップS18, S32）、これを配布することとした（ステップS19, S32）。その代わりに、情報端末103自信が復号して得た平文を受信端末103の暗号鍵（公開鍵）で暗号化したもの

10 を暗号化配布情報として配布しても良い。

【0114】また、図5、6、8、9のフローチャートに示される手順は、適宜修正して実施することが可能である。以上のように、上述した情報配布方式により、任意の情報端末103は情報供給局101もしくは他の情報端末103から所望の情報を取得できる。

【0115】次に、各情報配布方式による情報配布システムにおいて、有料情報の取得（あるいは情報の視聴）および有料情報の2次使用に対してどのようにして課金すればよいかを説明する。

20 【0116】図4に示した第1の情報配布方式では、情報供給局101からの配布以外に情報端末103同士での配布が行なわれるため、統一的に課金するためには各情報端末103に内蔵されている課金モジュール201にて有料情報の復号行為をカウントし、有料情報の復号の度に課金する方法が良い。

【0117】さらにその拡張としては、最初に一度復号するときだけ課金され、同じ情報の2度目以降の復号に対しては課金しないようにすることも可能である。これは、例えば一度復号した暗号化配布情報のシリアル番号を課金モジュール201内にリストとして保存しておくことで実現できる。

【0118】なお、情報供給局101は課金には直接結び付かないが、情報配布の記録を残しておくことで、その記録を不正端末の発見等に利用することができる。一方、図7に示した第2の情報配布方式では、有料情報を視聴するためには必ず情報供給局101から暗号化配布鍵を得る必要があるため、この行為を情報供給局101で記録すれば、有料情報の供給行為に対する課金を行なえる。すなわち、一度配布された情報は何度復号しても一定料金とするものである。

【0119】なお、情報端末103内蔵の課金モジュール201を利用すれば有料情報の復号の度に課金する行為も可能であり、情報供給局101では暗号化配布鍵の発行の記録は残すものの、情報の配布は無料とし、課金はすべて情報端末103内蔵の課金モジュール201に委ねることもできる。すなわち、暗号化配布鍵を受けとっても、それを利用しない限り課金しないこととする。

【0120】なお、有料情報の2次使用は、第1の情報配布方式および第2の情報配布方式のいずれの場合においても、課金モジュール201の処理によって行なう。

ここで、図4に示した第1の情報配布方式と図7に示した第2の情報配布方式では、各情報端末103には固有の秘密鍵が格納されており、しかもその秘密鍵の内容は情報端末103のユーザに対して秘密にされている。ただし、ユーザ端末103内に課金管理を行うモジュールが存在するため、悪質なユーザによりそのモジュールが攻撃され秘密鍵が漏洩する可能性がある。図7の第2の情報配布方式のシステムにおいて仮に、情報端末#xの秘密鍵K_xが漏洩したものとしよう。このとき、その秘密鍵K_xを用いることにより、情報端末#x用に配布された情報を監視聽できる。しかしながら、他の情報端末用に配布された情報は、秘密鍵K_xでは復号できないので、監視聽することは不可能である。すなわち、本方式では、たとえ特定の情報端末の秘密鍵が漏洩したとしても、任意の情報を監視聽できるわけではなく、被害がシステム全体に波及することはない。

【0121】また、情報供給局101に対して情報端末#xを装って任意の情報の配布を受けることもできるが、このようにすると、情報供給局101に記録される配布のログと、実際の情報端末#xから回収される利用記録のログから不正が発覚し、情報端末#xから秘密鍵K_xが漏洩したことが判明する。このような場合には、秘密鍵K_xを使用不能とし、情報端末#xの鍵K_xを更新すればよい。

【0122】このように、情報端末103の鍵を個別化したことにより、システムの健全性が大きく向上する。この点に関しては、図4の第1の情報配布方式のシステムでも同様である。ただし、このシステムでは、2次配布は情報供給局101の介在なしに実行されるため、情報供給局101のログだけでは不十分である。2次配布が行なわれた場合、その事実を送信側の情報端末103と受信側の情報端末103の両方に記録するようにし、それらの利用記録を先に述べたような方法で回収することにすればその記録をたどることにより不正を確認できる。

【0123】その後の鍵の無効化と更新は、先のシステムの場合と同じである。ここで、上述した各情報配布方式では、情報の1次配布および2次配布に慣用暗号方式を用いたが、その代わりに公開暗号方式を用いても同様の効果が得られる。この場合、受信端末103が暗号化配布情報を復号する際に必要な復号鍵（秘密鍵）のみを配布鍵とし、情報供給局101は、これを受信端末103に固有の暗号鍵（公開鍵）で暗号化した情報を該受信端末103に送れば良い。

【0124】また、前述したように、各局101、103、104間での情報の伝達には、どのような形態のメディアを利用して良く、本実施例で用いた通常の通信回線の他に、放送や記録媒体（例えばCD-ROMやフロッピーディスク、メモリカードなど）を利用することも可能である。なお、この場合の各局の構成は明らかで

るので、詳細な説明は省略する。また、本発明は上述した各実施例に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【0125】

【発明の効果】本発明に係る情報配布システムによれば、各情報端末には固有に暗号鍵・復号鍵を固有に割当て、配布するデジタル情報には固有に暗号鍵・復号鍵を割当て、デジタル情報は固有の暗号鍵で暗号化したものを作成し、これに必要な復号鍵を受信端末に固有の

10 暗号鍵で暗号化して配信するので、著作権を保護しつつ、デジタル情報の配布を情報供給局から行なうばかりでなく、既に情報供給局から配布を受けている情報端末からそうでない情報端末へも2次的に配布することが可能である。また、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその端末装置以外に及ばず、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。

【0126】また、配布された有料の情報の編集などの2次使用に対しても課金を行うことができる。一方、本

20 発明に係る情報配布方法によれば、情報端末には固有に暗号鍵・復号鍵を固有に割当てられ、配布されるデジタル情報には固有に暗号鍵・復号鍵が割当てられ、デジタル情報は固有の暗号鍵で暗号化したものを作成し、これに必要な復号鍵を受信端末に固有の暗号鍵で暗号化して配信するので、著作権を保護しつつ、情報端末では、デジタル情報の配布を受けることができるばかりでなく、既に配布を受けている情報端末から他の情報端末へも該デジタル情報を2次的に配布することが可能である。また、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその端末装置以外に及ばず、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。

【図面の簡単な説明】

【図1】本発明の一実施例に係る情報配布システムの概略構成を示す図

【図2】同実施例における情報端末の構成例を示す図

【図3】同実施例における課金モジュールの構成例を示す図

【図4】本発明の一実施例に係る第1の情報配布方式を説明するための図

【図5】同方式における1次配布手順のフローチャート

【図6】同方式における2次配布手順のフローチャート

【図7】本発明の一実施例に係る第2の情報配布方式を説明するための図

【図8】同方式における1次配布手順のフローチャート

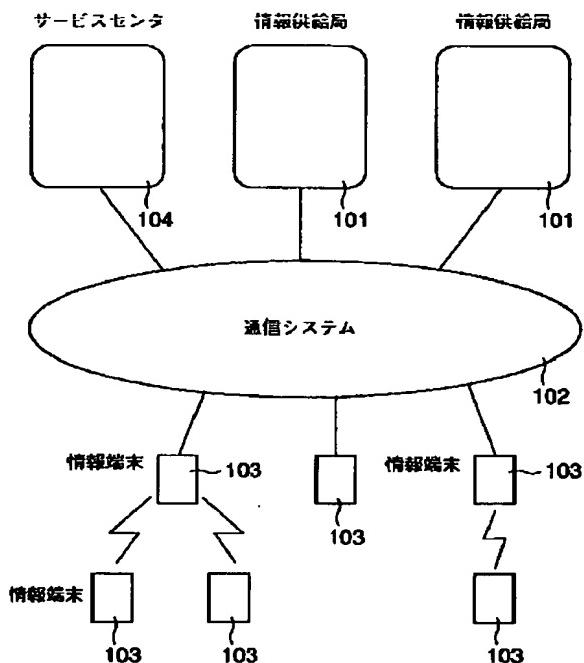
【図9】同方式における2次配布手順のフローチャート

【符号の説明】

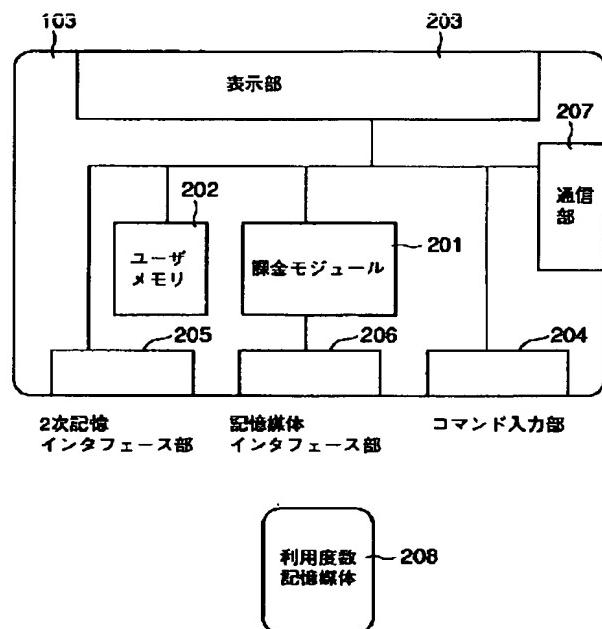
101…情報供給局、102…通信システム、103…情報端末、104…サービスセンタ、201…課金モジュール、202…ユーザメモリ、203…表示部、20

4…コマンド入力部、205…2次記憶インターフェース部、206…度数記憶媒体インターフェース部、207…通信部、208…利用度数記憶媒体、301…実行制御 *
 * 部、302…暗号器／復号器、303…健記憶部、304…課金管理部、305…保護メモリ

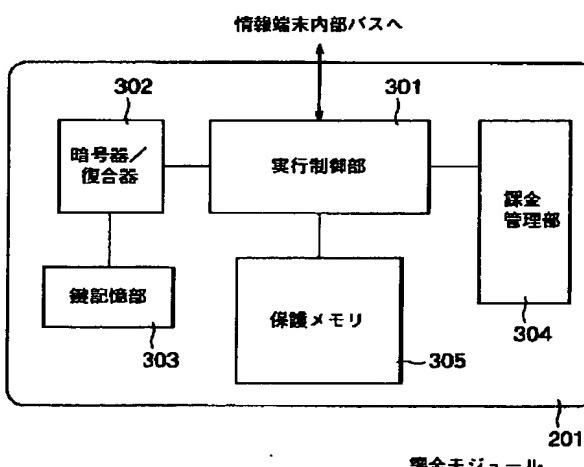
【図1】



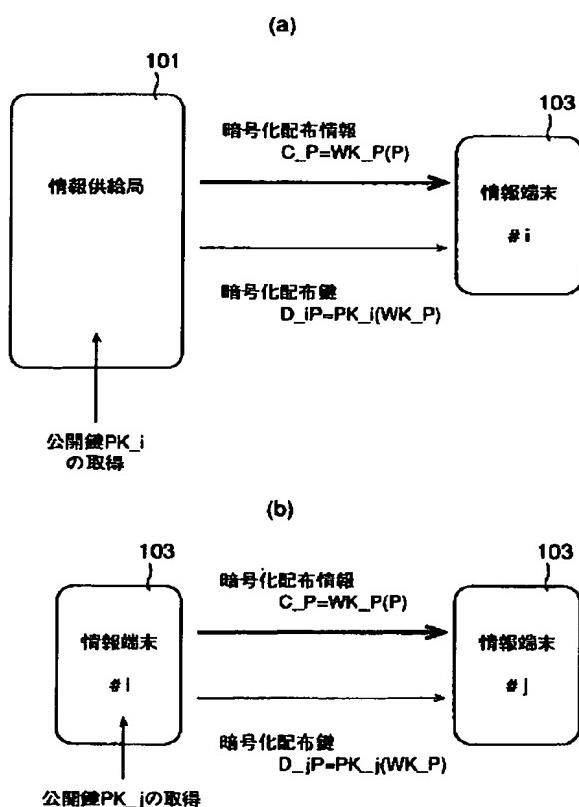
【図2】



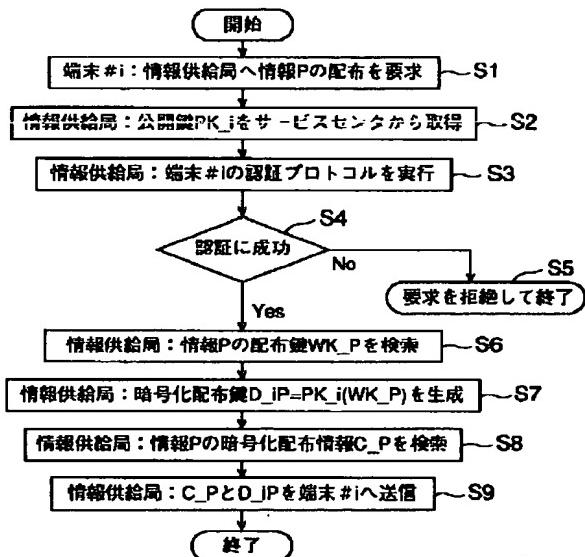
【図3】



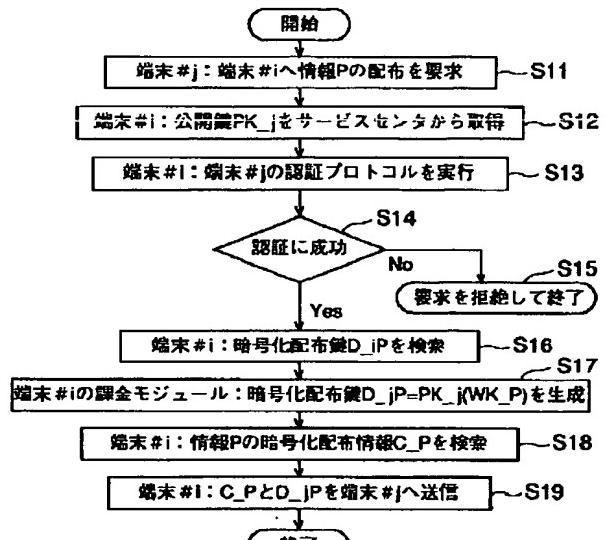
【図4】



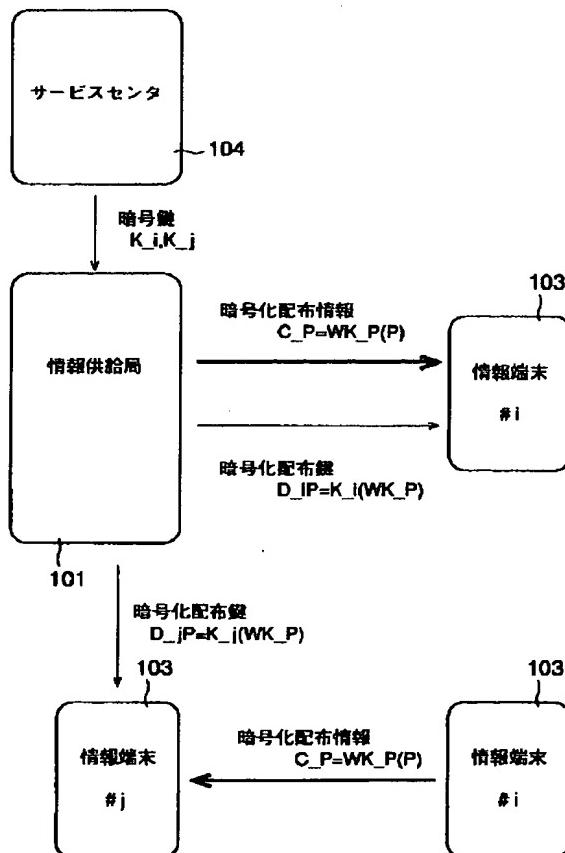
【図5】



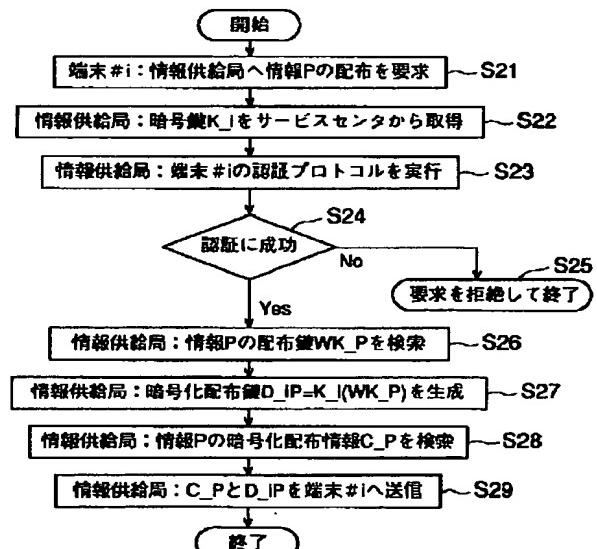
【図6】



【図7】



【図8】



【図9】

